工業控制系統之安全攻擊報告與防護策略

Security attacks on industrial control system

IBM Security

隨著工業 4.0、物聯網 IoT、智慧製造概念的崛起，產業界已開始落實製造自動化，提高營運效率。無論是軟硬體的虛實整合，或機台與機台之間的相互串連，「智慧化」整合都已成為新世代工業自動化系統的必要機制。

不過，既然工業自動化與智慧化引入資訊與通訊科技，資安威脅自然也隨之而來。工業生產設施、物聯網 IoT、以及關鍵的產業基礎設施，成為駭客新一波鎖定攻擊的目標。

- *天價等級的工業資安損失事件真實上演！*
- *知易行難：為何生產環境的安全防護出現漏洞？*
- *工業資安不只是「工廠資安」*
- *工業控制系統的安全防護 ABC*
- *面對工業資安挑戰，台灣產業應有的態度*

一堂要價數十億元學費的資安課

近期一家世界級的高科技公司，不慎讓病毒在廠區擴散，生產線被迫停機檢測數日，造成的出貨延遲、營收短少等影響，預估達新台幣數十億元之譜。對這家公司來說，金錢損失事小，商譽受損才是天大的打擊！除了立即與下單客戶密切協商新的交貨時程，儘快追上進度之外，CEO 更得親率高階主管站上第一線，對監管機關、分析機構與媒體解釋事件始末和處理進度。可見工業資安威脅已經站上檯面，造成實際的傷害。

工業資安現況與挑戰

雖然此次事件直接的肇事原因，指向廠區安裝人員沒有按照 SOP 執行病毒檢測，就把新機台接上廠區內部網路，造成病毒擴散。但其呈現的背後結構性問題，正是 OT（Operational Technology）領域，也就是工廠生產製造系統的安全防護難題。

對製造業而言，常認為只要將工廠生產系統的網段切開，與辦公 OA 網路及外部 Internet 隔離，加個防火牆，就能免於攻擊威脅。

但怕就怕禍起蕭牆之內！現今仍有許多基於 Windows XP / Windows 7 舊版作業系統的機台設備在生產線上運行。基於生產線穩定性的考量，這些機台設備多半保持當初導入時的設定，不敢輕易將作業系統升級，也未能落實安裝最新的漏洞修補程式，形同毫不設防。一旦攻擊感染源有機會侵入生產網路內部，反而更能恣意肆虐，一發不可收拾。

那，為什麼廠區內的 OT 機台設備，不能像 IT 管理辦公 OA 環境那樣，及時安裝該有的修補程式呢？

OT 思維 vs. IT 思維

這肇因於 IT 與 OT 的不同思維：
現今 IT 領域的軟硬體系統幾乎已經標準化，只要修補檔釋出，IT 部門人員就可開始透過標準化的機制快速進行更新，力求防堵最新的攻擊。而且辦公室環境的系統可以允許軟體升級、補強安全漏洞，以及安裝許多資安工具軟體來進行系統監控。甚至在萬不得已的情況下，對於強迫系統重開機這類狀況也有較大的容忍彈性。

OT 部門的責任卻是確保生產線穩定運作，恨不得 24 小時不停機，謀求生產效率的極大化，在沒有必要的情況下是毋須變動，也幾乎不允許變動。況且過往針對 OT 領域的資安威脅並不大。在這樣的前提下，若為了資安目的，時常將機台設備停下來更新修補程式，對生產效率帶來的負面影響，遠大於系統被攻擊的潛在風險。

更進一步說，就算想對 OT 設備進行安全更新，也不是一件容易的事。

當初採購機台設備時，往往是軟硬體整套購買，包括內部應用軟體、周邊硬體和作業系統。不同廠牌的機台設備常有特殊規格的硬體 / 韌體元件，其驅動程式只能由原供應商提供，連搭載的作業系統也可能是廠商特製過的嵌入式版本。

背後結構性問題，正是 OT（Operational Technology）領域，
也就是工廠生產製造系統的安全防護難題。

為了避免影響設備的效能或功能，以及保固的考量，供應商甚至會鎖死 OS 權限，禁止客戶自行再安裝其他軟體或工具。即便機台搭載的作業系統已釋出新的修補檔，仍須依賴原供應商來安裝調整，由他們確保作業系統 / 驅動程式 / 應用程式間的相容性，才能劃清更新之後機台正常運作與否的責任歸屬。

萬一當初的設備供應商已經不再為早期機台設備提供技術支援，甚至是供應商公司已經停止營業，那 OT 部門就只能勉力維持現狀，不敢輕舉妄動。若是 IT 部門貿然對 OT 的機台設備動手更新卻出包的話，這責任可是任誰也扛不起的。

工業資安 不只是工廠生產環境的事

其實，工業資安攻擊不只出現在工廠生產環境，也發生在實際運轉中的基礎設施系統，甚至是人們日常生活中使用到的智慧化 IoT 設備之中。

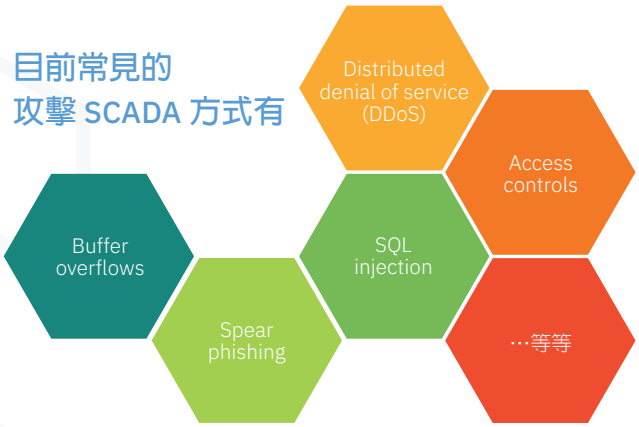
2010 年，伊朗位於 Natanz 核設施工廠的西門子自動化設備被植入了 Stuxnet 病毒，控制了提鍊濃縮鈾的離心機，表面上回報狀況正常，實際上卻操控離心機使其高速運轉而損壞，也因此導致伊朗 Buschehr 核電廠啓動時程延誤數月之久。

2015 年，克萊斯勒汽車傳出 Jeep Cherokee 越野車存在安全漏洞，駭客可入侵無線通訊系統，不但能隨意調控冷氣溫度、收音機音量以及雨刷等功能，還能操控方向盤及控制車速、追蹤行車路線。克萊斯勒被迫耗費巨資召回在美國售出、裝設有“uConnect”系統的 140 萬輛車，並對軟體進行更新。找出該漏洞的網路安全專家 Charlie Miller 則發文嘲諷：「到底是把車輛設計得更安全比較便宜？還是出事後才將車輛召回比較便宜？」

工業資安的基礎 ABC

想做好工業資安，當然應該徹底了解工業界的現況與常見的挑戰，方能對症下藥。在此我們特別要推薦一篇報告：**《Security attacks on industrial control systems 對工業控制系統的安全攻擊》**，該報告分析了對工業界的 ICS（工業控制系統）、SCADA（資料蒐集與監控系統）、PLC（可程式邏輯控制器）常見的攻擊手法，並建議完整的防禦之道。

對現代 SCADA 系統攻擊的途徑，首先可透過人工，或是讓 SCADA 控制主機感染病毒，去植入未經授權的控制程式。再來是對 SCADA 設備所在網段的通訊封包下手，因為 SCADA 使用的控制協議不具備加密機制，這可以讓攻擊者透過發送命令去控制 SCADA 設備。



對保護 ICS 系統而言，重要的防禦方向包含了：

1. 詳細定義 ICS 相關的網路架構、應用程式、資料庫等等
2. 阻絕任何可能的外部的侵入途徑，包含不安全的磁碟機、USB埠、無線網路、第三方網路等等
3. 加強存取控制，除非經過事先允許，否則不應該容許任何外界網路接觸到 ICS 網路
4. 使用點對點IPSec或SSL技術，通過VPN保護所有遠程訪問
5. 管控 ICS 功能，只留下最必要的，減少出錯機會
6. 部署縱深防禦安全方案，例如威脅管理與下一代防火牆等方案
7. 針對 ICS關鍵應用部署監控和日誌記錄
8. 管理並記錄所有的配置更改
9. 定期監管
10. 定期備份，建立快速回復機制
11. 導入 Intrusion detection and prevention system (IDPS) 解決方案

台灣產業對工業資安應有的對策

電子資通領域與自動化機械乃是台灣科技與製造業的強項，實不能輕忽工業資安對明星產業可能造成的危害。藉由近期這個事件，反而是重新審視工業資安威脅的契機。

台灣的產業切不可只求短線解決「工廠資安」的問題，應思考如何從源頭的產品設計、中間的生產環境、到後期產品實際應用情境，都將安全防禦思維融入其中，同時為攻擊造成損害之後應採取的事件回應 SOP 預作準備，才能從工業體系全局考慮整體的安全策略，將可能發生的威脅損失降至最低。

閱讀完整報告

想詳細了解工業控制系統的安全防護策略嗎？我們推薦您下載閱讀完整的《**Security attacks on industrial control systems**》報告，希望對您制定工業安全戰略，有所助益！

與我們連繫

若您有任何與 IBM 資安情報、資安產品或資安服務等疑問，歡迎您來電 0800-016-888 按 1，或前往 **https://www-03.ibm.com/security/tw/zh/** 與線上業務代表互動。

工廠資安無法短線解決，從源頭的產品設計、中間的生產環境、後期產品應用情境，皆必須融入安全防禦思維，同時為安全事件應變做好 SOP 準備，以管理安全風險。